The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS, INFORMATION WARFARE: POLICY PERSPECTIVES AND IMPLICATIONS FOR THE FORCE

BY

LIEUTENANT COLONEL MICHAEL J. STEWART
United States Army

USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS, INFORMATION WARFARE: POLICY PERSPECTIVES AND IMPLICATIONS FOR THE FORCE

By

Lieutenant Colonel Michael J. Stewart

Mister Bob Minehart
Project Advisor

US Army War College
Carlisle Barracks, Pennsylvania 17013

THIS PAGE LEFT INTENTIONALLY BLANK

ABSTRACT

AUTHOR: Michael J. Stewart (LTC), USA

TITLE: Information Operations, Information Warfare: Policy Perspectives and Implications for the Force

FORMAT: Strategy Research Project

DATE: 15 April 1997 PAGES: 34 CLASSIFICATION: Unclassified

Information Operations and Information Warfare are hot topics today and as a result, there is a tremendous amount of intellectual capital invested in the debate over what impact of new information technologies will have in two areas. These areas parallel two of our three components of the national security strategy; first is enhancing our security and the second is promoting prosperity. In many regards, the interests involved are somewhat mutually exclusive, which presents a challenging environment for issue identification and policy development. This paper identifies a few of the many scenarios in which information operations/warfare are a component; reviews some of the directions provided to the government as a whole and the military in particular; discusses why our nation is now more vulnerable to asymmetric attack; and then provides a few historical precedents. Finally, several of the many issue areas are analyzed, followed by the derivative implications for our military forces. The basic philosophical underpinning in this analysis is that solutions to these emerging issues must be consistent with our historical identity and values; failing this, we expose our long-term interests to unacceptable and probably fatal risk.

THIS PAGE LEFT INTENTIONALLY BLANK

TABLE OF CONTENTS

THIS PAGE LEFT INTENTIONALLY BLANK

List of Illustrations

THIS PAGE LEFT INTENTIONALLY BLANK

" BUT IF THE WATCHMAN SEES THE SWORD COMING AND FAILS TO BLOW THE WARNING TRUMPET,..., I WILL HOLD THE WATCHMAN RESPONSIBLE..."

Ezekiel 33:6

Introduction

Over the past several years our nation and the world have experienced a growing sense of possibility and creative potential as we transition from the industrial age to an information age. These trends have been fueled by significant advances in information technologies. Emerging technologies have also increased the fundamental vulnerability of our nation, as our economic and social infrastructure grow ever more reliant and increasingly dependent on information-based processes and systems.

These parallel but contradictory perceptions of opportunity and vulnerability have resulted in much intellectual and practical effort by individuals, private organizations, and governmental agencies to make sense of this new world. It is a dynamic environment, but perhaps captured by the technological aspects of what is fundamentally an enduring phenomena.

Information, knowledge and influence present our nation with perhaps its most troubling challenge since the end of the Cold War. At issue is whether we face a revolutionary paradigm-shift, requiring completely new national values and the derivative ways, concepts and policies to deal with a renaissance world, or if the bedrock qualities and values of our nation remain relevant and sufficient to deal with these challenges. This paper will address some of these issues in the context of historical example, argue

that our enduring values remain valid, and then discuss the derivative implications for our military forces.

Information Warfare In Context: Information Operations

What is this thing called Information Warfare? Is it a futuristic, Buck Rogers-type war which has arrived today? Or is it something more subtle and enduring? Reflecting the early stages of development, the terms information operations (IO) and information warfare (IW) (IO/W) is used by a wide variety of political, military, and economic leaders in a wide variety of contexts. As a result, it is overworked and underdefined; as a consequence, it means everything and nothing. Some commentators have attempted to refine and distill this variety of contexts. For instance, Arquilla and Ronfelt have coined the terms 'cyberwar' for internetted conflict in the military realm, and 'netwar', a societal-level conflict across the spectrum of the economic, political, and psychological makeup of a nation.[1] These efforts at achieving definitional precision are complicated by the tremendous market and political pressures to develop and exploit these very systems as a means of increasing market access and individual, national, and global prosperity. For the purposes of this paper, I'll use the term Information Operations/Warfare (IO/W) to cover the breadth of this concept.

It is useful to consider a few examples to appreciate the broad range of circumstances in which information, knowledge, and decisionmaking play a significant role.

In March 1995, the commanding general of the First Cavalry Division, was speaking with several of his subordinate commanders about the upcoming Battle Command Training Program (BCTP) Warfighter Exercise (WFX). He said that this battle, as well as any other battle, was a contest of wills between the opposing commanders. These comments were profound in their simplicity and comprehensiveness; only through the effective use of information could he achieve the dominance over his adversary. As a consequence, every activity must support the destruction of the enemy commander's will and ability to fight. In the words of Sun Tzu:

> "All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are near. Offer the enemy a bait to lure him; feign disorder and strike him. When he concentrates, prepare against him; where he is strong, avoid him. Anger his general and confuse him. Pretend inferiority and encourage his arrogance."[2]

Here is another example of information use in a mostly military context, although it also shows the web existing among each element of national power. Larry Bond's fictional but very realistic *The Enemy Within*[3] provides an exceptional description of information operations in support of strategic objectives. The story concerns an Iranian rapprochement with the US, designed as a grand deception. The purpose of the deception is to paralyze the US through foreign agent-induced racial unrest, rendering the nation incapable of responding to a Persian offensive to seize Arabian Peninsula oil fields. The point of this is that this operation wasn't an "information operation" but many information operations, or tools, designed to achieve vertical strategic/operational/tactical coherence, toward a grand objective.

IO/W is not limited to military matters. Economic espionage has become a hot topic of debate since the collapse of the Soviet Union, as nations look to national self-interest and domestic prosperity. Several nations, notably France,[4] reputedly the most neo-mercantilist, and Germany, Switzerland, South Korea, Israel, China and others, are alleged to conduct state-sponsored economic espionage. Both the FBI and the CIA consider economic espionage as a current, ongoing threat that will continue to develop with time.[5]

Even our domestic environment is subject to information operations of many different types. On one level, our leadership at all levels work hard at providing an image of our nation that supports and insures "the domestic tranquillity". Most of us can recall some event which necessitated a public address by a governor, some national figure, or even the President. These events occurred to assure the American people in general, or an interest group in particular, that all was well or would be well soon. This is evident after some extensive natural disaster, domestic rioting, or significant international event.

On yet another level, partisanship and interest group influence are framed by the recent disclosures and ongoing debate of campaign finance irregularities by the Democratic National Committee (DNC). This includes the alleged improprieties of coffees and overnight stays in the White House. The facts and allegations are complicated. In short, it appears that the Lippo Group, an Indonesian transnational corporation, with business interests in mainland China, may have gained undue influence through John Huang's election campaign fund-raising efforts. Huang is a former employee of Lippo working in the Department of Commerce at the time. Yet another

possibility is that US trade negotiating positions may have been compromised, again through Huang. These sorts of reports also highlight the bridging nature of these events between our domestic and international environments.

IO/W can cover a lot of ground - economic, political, and military - domestic and international - governmental and corporate. It is also apparent that while electronic means present new vulnerabilities, old style influence-peddling or buying maintains a prominent place in the world.

Professor George J. Stein provides a useful capstone perspective, which recognizes that information is a means to an end:

> "Information Warfare, in its largest sense, is simply the use of information to achieve our national objectives. Like diplomacy, economic competition, or the use of military force, information in itself is a key aspect of national power and, more importantly, is becoming an increasingly vital national resource that supports diplomacy, economic competition, and the effective employment of military forces. Information Warfare in this sense can be seen as societal-level or nation-to-nation conflict waged, in part, through the worldwide internetted and interconnected means of information and communication."[6]

His key point is that information is leveraged in a variety of ways to achieve national objectives. Just as any other resource, it is used effectively or ineffectively. Information is the essential component of decisionmaking - - precision and ambiguity count. Effective use of information during decisionmaking is manifested by seizing and maintaining the initiative, whether it be in domestic politics, international diplomacy, economic competition, or military operations.

Complicating this environment is the phenomena of "compression", described by Doug MacGregor. Information technology advances have provided opportunities for military leaders at all levels to share an increasingly common view of the battlefield, unimaginable even ten years ago. As a consequence, the distinction between the levels of war dissipates.[7] We should anticipate a similar experience within the other elements of national power. Continuing to follow his logic, not only will we experience continued vertical compression in the military and other elements of power, we will also see increasing horizontal compression among the elements of power.

Elements of National Power			
Economic	**Political**	**Diplomatic**	**Military**
Strategic	Strategic	Strategic	Strategic
Operational	Operational	Operational	Operational
Tactical	Tactical	Tactical	Tactical
Informational Support Activities			

Figure 1: A Matrix for the Elements of National Power and Levels of Activity

This means our activities, whether they be military, economic, diplomatic, or political, must be more consistent and coherent than ever before. Not only does emerging

technology help us achieve this, but it provides a very large and significant window for the rest of the world to watch and learn from our every move. If we want the world to follow our lead, embracing democratic ideals and free markets, we must set the example, continuing to embrace our traditional values, democratic ideals and free markets. Does adequate strategic structure exist to set the conditions for success in such a world?

National Directions for Information Operations/Warfare

The world and our nation are in the throes of fundamental change in the international order, economic competition, and the medium of conflict. At the heart of this change is the concurrent, interrelated, and accelerating pace of technology in the fields of telecommunications, both television and telephone, computers, and information services. Coupled with the collapse of communism and the general trend toward market economies, this environment has produced significant challenges to the basic economic, military, political, and psychological vitality of our nation. It has been described as a "clear and present danger" by Director of Central Intelligence John Deutch, in July 1996:

> "... The US will face very, very large and uncomfortable incidents at the hands of cyberterrorists...The US government is not well-organized to address the threat of foreign attacks on public switched networks and government systems..."[8]

There are a number of discussions, reports, and initiatives focusing on the vulnerabilities of the infrastructure which supports our way of life - communications, power, transportation, water, oil and gas control, media, civil works, financial, and governmental operations. A recently published document by the Defense Science Board Task Force on Information Warfare (Defence)[9] lays out a comprehensive assessment of

our vulnerabilities, associated legal issues, and recommended remedial actions. It calls for "extraordinary action" to deal with emerging IO/W techniques and tools, while ruefully noting that this is the third year running that such a Defense Science Board panel has made such recommendations.

Our *National Security Strategy of Engagement and Enlargement 1996* provides the latest high-order vision which ultimately drives our implementation of IO/W concepts. Facilitating this strategy of engagement and enlargement are three major components: enhancing our national security, promoting domestic prosperity, and promoting democracy abroad.[10] Each of these components plays a critical role in advancing our national interests in what is, in effect, the competition of ideas. The basis of world class competition in the realm of ideas rests upon the capacity to use information as a means to win the idea race. In military operational terms, this is described as information dominance[11] and it applies across the spectrum of national activities designed to achieve the stated strategic components.

This document sets clear objectives for the use of various information tools and techniques particularly in enhancing security and more generally in promoting prosperity and democracy. For example, the intelligence community is tasked to "to gather timely intelligence on current and emerging information technologies or infrastructure that ... threaten US interests"[12] and "supporting the development of protection strategies."[13] Significantly, this document also recognizes that national emergency preparedness is a critical piece of a defensive effort as the following extract demonstrates:

> "We will do all we can to prevent destructive forces such as ... threats to our information systems ... from endangering our citizens. But we must also be prepared to respond

> effectively if an emergency does occur in order to ensure the survivability of our institutions and national infrastructure, protect lives and property, and preserve our way of life. National security emergency preparedness is imperative, and we must continue to work aggressively to ensure appropriate threat mitigation and response capabilities... To this end, comprehensive, all-hazard emergency preparedness planning by all Federal departments and agencies continues to be a crucial national security requirement."[14]

Our national objectives are clear - - increase our nation's prosperity (and coincidentally that of the other members of the world economy), as well as promoting democratic processes and institutions, through aggressive exploitation of the Global Information Infrastructure (GII), while protecting our National Information Infrastructure (NII) and Defense Information Infrastructure (DII).[15]

Although not as current as the national strategy document, our *National Military Strategy 1995* (NMS) document likewise presents a balanced emphasis on IO/W as a supporting concept of the national military objectives of promoting stability and thwarting aggression.[16] Each of the three supporting components, peacetime engagement, deterrence and conflict prevention, and fight and win, is supported in turn by a number of enabling activities. Many of these activities contain some form of informational content, providing a wide variety of "platforms for imparting influence and democratic values"[17] as envisioned in the NMS document.

The Department of Defense has also released a strategy paper, *Information Warfare* which expands on the basic concepts in the *National Military Strategy* document. Perhaps the most significant element in this particular document is that it

IO/W for society as a whole. It underscores the importance of synchronizing all elements of national power:

> "...IW at both the national-strategic and theater-strategic levels requires close coordination among a wide variety of elements of the USG, including the Department of Defense."[18]

The latest Secretary of Defense *Report to the President and the Congress* makes much the same point. It recognizes that IO/W has the potential to expand significant, damaging conflict well beyond the traditional boundaries of a conventional military fight:

> "*The importance of information warfare (IW) extends far beyond military operations....* Virtually every facet of American life is affected by electronic media - television, radio, banking, communications, and service industries. Each of these, in turn, affects national security."[19]

If there is a shortfall in the national level focus and direction for our IO/W strategy, it lies in the apparent absence of any corresponding, parallel documentation by the other Cabinet-level Departments. That is not unusual however; there have been few, if any, like publications in any of the other functional areas, although it is likely that the Federal Emergency Management Administration (FEMA) does develop and maintain some level of operational documentation.

Asymmetric Challenges to US National Power

Based on recent successes by the US military, an adversary, be it nation or non-nation, in pursuit of its objectives, will likely choose an asymmetrical tool with which to challenge US power.[20] By test, our military forces are the best in the world, with no near-

competitors. Our capabilities demonstrated during Operation DESERT STORM and since have convinced many in the world to pursue other means of conflict. Information operations provide an capability for our enemies to attack us asymmetrically. This effectively avoids our demonstrated strengths in a conventional fight, and threatens a relatively vulnerable center of gravity, a source of strength and vitality. It is also a very inexpensive option, well within the budget of an extremely broad range of adversaries.[21]

These foes, real and potential, range from rogue nation-states such as Iraq, Iran, Libya, North Korea, and others, to individuals such as zealots in the image of domestic mail-bomber Ted Kacynski, and common criminals, to business entities seeking commercial advantage. More importantly, the target set will not be restricted to military infrastructure and forces; our commercial, financial, service, educational, and all other critical infrastructure resources are at risk. Asymmetric engagements will test our strategic agility in coordinating, collaborating, and synchronizing all our elements of power - military, economic, political, and psychological. Given the low entry cost and enormous potential weapon's effects, this media could become the "poorman's" weapon of mass destruction of choice.

Historical Precedents

Past experience is a useful starting point for discussing the range of options and justifications available to the policy-makers as they wrestle with the issues associated with emerging information technologies.

A very good example is the case of Franklin D. Roosevelt, thirty-second President of the United States. He was a very savvy politician who exploited the new technology

available to him - the radio - during his successful campaign against incumbent Herbert H. Hoover. Franklin Roosevelt continued to use the cutting-edge technology of the day in calming the nation, providing a vision of a better future, and generating support for the necessary implementing programs. Later, he would use similar talent and technology as he prepared the nation for a coming war.

Every administration since has used the available technology, along with proven, enduring tools, to communicate, and ultimately influence, the American people. In keeping with this trend, the Clinton administration has established a White House website.

The unwritten international code regarding espionage has been one of tolerance, perhaps even necessity. In the event that some aspect of the espionage game came to the public's attention, administration rhetoric was ratcheted up for domestic consumption and perhaps an attache or two would be expelled but otherwise little concrete reaction occurred. While theft of state secrets was guarded against, the international order recognized this as acceptable activity engaged in by everyone against everyone else, friend and foe alike. However, it's worth considering whether this tolerance would be present if say, the secrets stolen provided the ability to defuse the nuclear arsenal of the other side, in effect, destabilizing the strategic balance.

In a slightly different context is open source information collection. The Central Intelligence Agency performs this function through a program called the Foreign Broadcast Information Service (FBIS).[22] The FBIS routinely records and translates thousands of radio broadcasts, making speeches and other public record documents of

foreign representatives available to academics, as well as intelligence and policy analysts. Not only can trends, both constant and changing, be discerned, governments can use this media as a way of signaling to the US government. More ominously, this can also be a potential barrier to crisis resolution, as it nearly was during the Cuban Missile Crisis, as described by Roger Hilsman.[23]

The terrorism campaigns of groups such as the Palestinian Liberation Organization (PLO) are yet another example. This high visibility violence was a tool to focus attention on the plight of Palestinians displaced by the establishment of the State of Israel and the subsequent capture of Arab lands during the several Arab-Israeli wars. These events were initially designed to target the Israeli public, but the PLO soon recognized that world opinion in general and US opinion specifically could provide an acceleration effect in persuading the Israelis to negotiate. The strategy embraced high profile events designed to capture maximum news coverage. That these information operation tools were effective is attested to by the ongoing negotiations between Yasser Arafat, the PLO leader whom Israeli leaders vowed never to deal with, and Benjamin Netanyahu, the Israeli hard-line, conservative Prime Minister. The Palestinians are establishing a homeland with the aid of Israel.

Yet another case is that of the USS Liberty, an intelligence collection ship, which was attacked by Israeli aircraft and torpedo boats, sustained heavy damage and suffered tragic loss of life during the '67 Arab-Israeli War. While the various participants paint significantly different pictures of how this happened, there is absolutely no question that the attack occurred. A US Navy ship in international waters was attacked by Israeli

armed forces; most US officials believed the attack was deliberate with the objective of denying US access to electronic intelligence on Israeli operational plans. In this scenario, the Israelis acted in order to introduce ambiguity in the US decisionmaking cycle. This was to further delay any US attempts to coerce Israel into a cessation of hostilities before Israel achieved its war objectives. Our response was limited to diplomatic protests.

During the Cold War, the US engaged in psychological operations against the Soviet Union, it's Warsaw Pact partners, as well as the Soviet's western hemisphere ally, Cuba. The tools used were Radio Free Europe and Radio Marti. These were radio broadcasts targeting the people, with the purpose of undermining the regimes in power by direct appeal to the subjugated populations. Likewise, these nations responded with information operations designed with similar purposes in mind. While neither side particularly liked the idea of these operations against them, it was essentially a quid pro quo situation; the activity was tolerated under the accepted rules of the game.

More ominous, yet less obvious, is the erosion of national culture and identity through the effects of the mass media and marketing. Canada is only the latest nation to bemoan the effects of "the American culture vulture", which countries worldwide believe is permeating an Americanized global culture.[24] The Director, Defense Intelligence Agency, emphasized this point in recent testimony before Congress. In turn, the US is concerned about the influx of Hispanics, a demographic trend which could eventually lead to unforeseen sea changes in how the US deals with itself and the world.

Policy Issues

Certainly the emerging technologies are mixing with the old order to present novel challenges to our strategic leaders. What is the proper US policy posture regarding the range of IO/W activities in peace, crisis, and war? Perhaps the single most important question is what actions within the umbrella of IO/W constitute an act of war?

Classes of Actors: Potential antagonists include nation-states, NGO/PVO's, interest groups, individuals, and transnational corporations. While the nation-state, as well as many transnational corporations, may possess the capability and the motivation to engage in information operations against the US, I believe that most, if not all, would attempt to limit the effects of the operation. Generally this class of actor has a vested interest in maintaining some semblance of today's economic system, as well as dynamic political stability. Their efforts would be directed to creating opportunities for a gradual, but cascading increase in their relative power vis-a-vis the US.

Similar comments can be made about the NGO/PVO's; these organizations have specific agendas and objectives, but generally speaking, these sorts of groups hold vested interests in a world approximating the one we know today.

Interest groups, such as the PLO, also generally hold a vested interest in the present world in a general sense, but possess very specific objectives which the world must accomodate, for instance, a Palestinian state. The PLO has used a number of tools to achieve its goal, attacking US interests to gain our attention and subsequently relying on US support to consolidate gains.

Individuals could possess the philosophy, capability, and intent to attempt to inflict large-scale damage to the integrity of the US. However, it is unlikely that an individual actor could threaten the survival of US, although it is also clear that significant damage is possible. On this scale, I believe we can apply sufficient resources to stem and staunch the damage in order to avoid a catastrophic cascading, deteriorating effects on our national interests.

Finally, transnational corporations (TNC) represent a hybrid of interests most at odds with the current system of nation-states. These corporations are fundamentally different than their counterparts of 20 to 30 years ago. Their interests transcend artificial political boundaries, instead following the contours of cyberspace and the flow of capital and markets. Increasingly, these TNC conduct collection operations and attempt to influence government decisionmaking. For instance, General Motors and Volkswagen recently settled a lengthy dispute, which arose from alleged trade secret theft by a former GM executive, hired away by Volkswagen. The ongoing campaign finance hearings also bear witness to this phenomena. The TNC also will be involved in counterintelligence activities as a result of other TNC efforts to collect information. In sum though, TNC still depend on the current global economic system, which would serve to limit, but not eliminate, the tendency toward damaging IO/W.

ISSUE: Information Theft. What will our response be to information operations in which theft or attempted theft of information is the intent and result? This falls into the category of simple espionage. Just as the Cold War actors recognized, these are a necessary component of international discourse. Certainly individual actors will receive

uneven treatment; those operating under diplomatic cover will never risk the same punishment that their recruited operatives will.

The very nature of information theft is transforming as a result of the INTERNET; formerly classified satellite imagery is now available, as are some relatively sophisticated designs for weapons of various types. The information that is targeted is financial data and money. Although these sorts of cases are best left to law enforcement agencies, there could come a time when perpetrators could threaten the financial stability of a nation.

We must also determine to what degree we are willing to ask or allow our government, corporations, and individual citizens to engage in like activity against other nations (friendly, neutral, benignly hostile, and actively hostile), other national and transnational corporations, and indeed, other nation's private citizens.

ISSUE: Information Attack. Information attack can take several forms. Several years ago terrorists exploded a bomb in the basement parking area of the World Trade Center. This kinetic attack targeted the financial operations located in the building. During the Vietnam War, the North Vietnamese employed propaganda tools designed to attack the American public's perception of the war. In a third medium, there have been increasing numbers of electronic tools or weapons employed which effectively deny computer service to legitimate users. Each of these represent assaults on information and decision processes; what is the appropriate response and on what framework is it based?

These scenarios each possess unique characteristics; however, the response to each must share the common core of our national character, history, and most importantly, our values. If we implement policies which can be interpreted as a

repudiation of these stated values, we risk the future to short-term matters of convenience.

ISSUE: **Influencing Decisionmaking.** The most notable case in this category is the ongoing investigation of 1996 campaign irregularities by the DNC. What is the best policy to apply in the case of foreign efforts, government and corporate, to influence our governmental processes? A free and open process of debate and Congressional review is our best defense against such efforts. This is no aberration from our national experience; the framers of the US Constitution designed a system that insures ambition will counter ambition. In this global environment, we should expect foreign ideas to compete with our domestic ideas; this is what our Founding Fathers envisioned.

ISSUE: Peacetime Offensive Information Operations. Our consideration to employ offensive Information Warfare weapons must be cautious. A decision to strike with such weapons must survive the test of time. A logical method to consider is our considered restraint in use of nuclear weapons. Is it in our national interest to conduct offensive information operations in peacetime? This involves balancing interests which may be mutually exclusive. For instance, the military interest in force protection would be consistent with inserting a covert virus in the electronic controls of a foreign weapon system, to be activated later if necessary. Likewise, similar tools targeting economic or political mechanisms might also be possible.

In contrast, our economic interests in a free and engaged world economy argue against such provocative activity. First, such activity would undermine our stated national strategy of engagement,[25] rendering our public diplomacy subject to suspicion

and ridicule, effectively undermining our long-term interests and objectives. These sorts of activities would also inhibit free-trade, one of our long-standing objectives on the road to national and world prosperity. Obviously, such activity would also encourage others to mimic these activities against our own information infrastructures.

Yet another reason to forego use and employment of such tools is the potential effects of an operation gone bad, in which the effects are commensurate with those of weapons of mass destruction (WMD), with probable spillover beyond political borders. This sort of activity is the rough equivalent of enactment of the Smoot-Hawley Tariff Act in the late 1920's; this legislation was a prominent precipitator of the Great Depression. Finally, if we accept such behavior as appropriate, I believe we risk potential politization of the decision.

ISSUE: Cultural Encroachment. Since the end of World War II, our Nation has enjoyed a position of unequaled economic prosperity. For this and other reasons, our cultural influence has permeated into nearly every corner of the world. Generally, we have not fully recognized the power and appeal of our culture and values; as a result, we have not been able to understand the concerns of other nations about the leaching effect of US culture. Our presence and interests are world wide and we field a wide array of bureaucratic instruments to achieve our objectives; among them are the USIA, USAID, and many others. Even the apolitical, stringently controlled Peace Corps is an instrument of cultural pollination. It is at least arguable that some part of Iran's demonization of the US results from a perceived cultural threat.

While other nations have expressed grave concerns about the influence American society has had on the world, US leaders are realizing that we aren't immune to this phenomena of cultural encroachment. Demographic trends, fueled primarily by illegal immigration, indicate that the US will be home to the world's fifth largest Hispanic population in the near future. I do not advocate pulling back from our traditional efforts to engage and influence the nations and peoples of the world; in fact, it is very doubtful that a government effort in this regard would be effective because of the transnational nature and extent of corporate and NGO/PVO presence in the world.

However, it is crucial that we recognize the validity of these concerns for several reasons. First, we only reduce our long-term ability to ultimately influence these other players if we continue to downplay or ignore their legitimate expressions of concern. Second, our public response to similar challenges in the US will be measured by other nations' in view of our responses to their challenges. Our policy must be consistent or we risk subjecting our national values and objectives to ridicule and suspicion.

ISSUE: Intelligence Support to Commercial Activities. This is perhaps the most controversial issue for the US intelligence community today - should our intelligence agencies be involved in economic espionage? On one hand, there may be a legitimate role for our counterintelligence resources to assist in safeguarding our corporations business secrets. However, even this role is fraught with danger as the nature of any corporate competition is convoluted by the transnational character of corporations. These entities are beholden to political allegiances less and to electronic commerce more.

Even more frightening is the prospect of active collection and subsequent passing to corporate representatives of trade secrets. This sort of activity would take us down a slippery path to a world in short supply of the qualities our national character espouses.

ISSUE: Information Attack Deterrence Strategy. Although there are many concepts that can be drawn from our experience with nuclear weapons, deterrence probably is not one of them. Our deterrence strategy against nuclear weapons was relatively simple: maintain a sufficient stockpile of like weapons with which to threaten an adversary's national survival. Possession of information weapons is not likely to deter the actors who would perpetrate such an attack on us. The nature of of the relationship is fundamentally different; our nation is more vulnerable to such attacks. An attacker is less vulnerable, and in most instances, significantly less vulnerable, to the point of invulnerability.

So how do we deter an adversary from attacking us in this way? Only through a proven, reliable, and demonstrated capability to detect, assess, and reconstitute whatever part of the NII is attacked and damaged. In an effort to reduce the risk of catastrophic failure, the government should undertake a civil defense program similar to that of the 50's and 60's, dedicated to developing and practicing responses to a variety of scenarios which assume successful IO/W attack.

> " ... Finally, deterrence in the information age is measured in the resiliency of the infrastructure than in a retaliatory capability."[26]

Implications for the Force

> "Therefore I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are certain to be in peril.'"[27]
>
> Sun Tzu

Our adversaries will increasingly favor asymmetric engagements to counter our conventional military power. This asymmetry will take many different forms and will greatly complicate policy-making and defensive IW. The Defense Science Board's recent report[28] questions any adversary's capability to plan a comprehensive information campaign against the US and achieve the cascading deteriorating effects necessary to achieve a catastrophic event. This seriously fails to account for the creativity available to those who hate us and wish us ill.

Our military forces have to recognize that the new tools provided by information technologies and the increased battlespace responsibilities require innovative doctrine, tactics, techniques, and procedures. We are on the right path; *Field Manual 100-6 Information Operations* is a milestone along this evolutionary journey. Joint doctrine is a little behind at this point,[29] but will build on Army doctrine and leap ahead, incorporating our latest experiences and professional judgments. Battlestaff procedures and techniques, however, remain an area in need of attention. In a recent article, John Stewart describes a product appropriate as a possible partial solution.[30] He calls for an overlay of the information battlespace as another Commander's Preparation of the Battlefield (CPB)[31] product. Applicable at any level of military operations or within any of the national

elements of power or in combination, this is an important concept. It is a starting point for our communicators, the J6's/G6's to lay down the friendly communications networks; our Public Affairs Officers to similarly build a graphic representation of PAO considerations; the Civil Affairs situation likewise displayed; and the intelligence J2's/G2's providing the parallel enemy products, as well as acting as the gatekeeper of the CPB process for the commander.

We must also recognize and anticipate requirements as a result of the compression phenomena described by Doug MacGregor. This compression effect is taking form vertically in stovepipe fashion for each element of national power, as well as horizontally among the power elements. The manifestation of this is already apparent in our use of military forces in humanitarian relief operations and peacekeeping operations. Yet another effort to leverage our military forces in asymmetric ways is the Partnership for Peace activities in Europe; these warriors are individual emissaries for our nation and our culture.

It would be prudent to designate Commander in Chief (CINC) Special Operations Command (CINCSOCOM) as the supporting CINC for all DOD offensive IO/W activities. A combatant CINC provides credibility, authority, and responsibility that intelligence and communications activities/staffs cannot.[32] USSOCOM has the staff and procedures in place that allow integration of these very sensitive capabilities into an overall operational scheme, supporting national objectives. Most importantly, these weapons would be under strict control similar to that provided nuclear weapons by Strategic Command (STRATCOM).

In keeping with the roles and functions associated with CONUS-defense and force-provider, CINC Americas Command (CINCACOM) should be designated as the responsible CINC for all DOD defensive IW activities, as well as the lead military command for national reconstitution planning, preparation, coordination, and execution, in coordination with other government agencies.[33] While FEMA is the lead federal agency for domestic disasters, it is appropriate and prudent that our military organizations develop the tools needed before such an event occurs.

As a first priority, CINCACOM should develop an operations plan supporting reconstitution of the NII, and as a parallel action, begin a series of seminars and exercises. These should build to the actual practice of reconstitution, in coordination with other national agencies. Until this is done, the element of risk exists at an unacceptable level. Additionally, based on past known and suspected attacks, we must assume that our networked systems have been compromised and remain so until "cleared and secured." These activities will require extensive effort and support from the NSA, DISA, and other agencies. It is probably appropriate to develop a joint doctrine, tactics, techniques, and procedures for this sort of effort.

The relatively low entry cost will expand the inventory of potential adversaries to a point nearly beyond comprehension. This could stretch our intelligence capabilities and other resources to the breaking point. Recently, according to open source material, the National Security Agency will establish a National Information Warfare Center as a watchdog for attack warning and assessment. This new organization will provide capabilities paralleling the FBI's Computer Investigative and Infrastructure Threat

Assessment Center (CITAC), which focuses on domestic computer crimes. The services have also established organizations and training programs designed to support defensive measures. These are steps in the right direction but we must insure that these efforts provide full-dimension protection and robust reconstitution capabilities. These efforts must be synchronized to cover the seams between services, between geographic CINC's, and vertically from tactical to strategic activities.

While the services possess extensive expertise in IO/W implications beyond the military element of power, there are efficiencies that can expand it. We must tap into the enormous pool of talent in the private sector software companies. Establish joint reserve component units as IO/W units; these units would recruit appropriately qualified members for defensive and regeneration functions. Someone like Bill Gates could be recruited to be a "colonel of the corps"; tapping into the civilian expertise would pay immense dividends. These sorts of units and members could establish partnership relationships with our various units and headquarters. This would assist in risk analysis and training to reduce those vulnerabilities. Senator John McCain has endorsed this sort of approach in his recent paper discussing the Quadrennial Defense Review.[34]

Conclusions

"A man's judgment is only as good as his information."
The Wall Street Journal

Information dominance, operations, and warfare are not new concepts. Nations, societies, interest groups, and individuals have long engaged in competition and confrontation using information and derivative knowledge to gain advantage over

competitors and defeat adversaries. Information and its use are constants throughout history. Certainly, historical case studies provide useful insights into the challenges of today, whether in issues of peace, crisis, or war; whether in domestic or foreign policy; and across each of the elements of national power.

New technologies are accelerating the effects of vertical and horizontal compression, as well as increasing opportunities for adversarial asymmetric attack. These are challenging times, but not so challenging that we should abandon the values which have made our nation what it is.

There are solutions to these challenges; these solutions lie in the ingenuity of good people adhering to the principles and precepts which have made our Nation great and a world leader. This approach supports our current national security strategy of engagement and enlargement, as well as creating the necessary environment for the supporting components of security enhancement, prosperity, and promoting democracy.

ENDNOTES

[1] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12 (April-June 1993), 145: available from http://www.stl.nps.navy.mil/c4i/cyberwar.html; Internet accessed 8 October 1996.

[2] Samuel B. Griffin, ed., *Sun Tzu: The Art of War* (London: Oxford University Press, 1971), 66-7.

[3] Larry Bond, *The Enemy Within* (New York: Warner Books, 1996). See also Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War*, (Santa Monica: RAND, 1996), which describes a similar scenario.

[4] Garth Hancock, "US Economic Intelligence Policy and Global Competition," Spring 1996; available from http://www.miis.edu/mreview/spring96/hancockart.html; Internet accessed 23 January 1997.

[5] Ibid., See also David E. Cooper, "Statement Before the Senate Select Committee on Intelligence on Economic Espionage: Information on Threat from US Allies" on 28 February 1996; available from http://nsi.org/Library/Espionage/allies.txt; Internet accessed 23 January 1997. This testimony confirmed allied espionage in economic matters but did not identify specific countries.

[6] George J. Stein, "Information Warfare;" available from http://www.cdsar.af.mil/apj/stein.html; Internet accessed 2 September 1996.

[7] Douglas A. MacGregor, "Future Battle: The Merging Levels of War," *Parameters* 22 (Winter 1992-93), 33-47.

[8] As quoted in *Signal Magazine*, (October 1996), 63.

[9] Office of the Secretary of Defense, *Defense Science Board Task Force On Information Warfare - Defense (IW-D)*, (DSB Report), (Washington: November 1996).

[10] The White House, *A National Security Strategy of Engagement and Enlargement*, (NSS), (Washington: 1996).

[11] Office of the Joint Chiefs of Staff, *The National Military Strategy of the United states of America 1995: A Strategy of Flexible and Selective Engagement.* (Washington: 1995); also see Office of the Chairman of the Joint Chiefs of Staff, *Joint Vision 2010*, (Washington: 1996); and Office of the Chief of Staff of the Army, *Army Vision 2010*, (Washington: 1996).

[12] The White House, *A National Security Strategy of Engagement and Enlargement*, (NSS), (Washington: 1996), 24.

[13] Ibid., 25.

[14] Ibid., 26.

[15] The White House, *Executive Order #12864: United States Advisory Council on National Information Infrastructure,* (Washington: September 1993); available from http://library.whitehouse.gov; Internet accessed 07 October 1996.

[16] Office of the Joint Chiefs of Staff, *The National Military Strategy of the United states of America 1995: A Strategy of Flexible and Selective Engagement*, (NMS), (Washington: 1995), 4.

[17] Ibid., 8.

[18] Office of the Chairman of the Joint Chiefs of Staff, *Information Warfare: A Strategy for Peace...The Decisive Edge In War.* (Washington: 1997), 5.

[19] Office of the Secretary of Defense, *Report of the Secretary of Defense to the President and the Congress.* (Washington: U.S. Department of Defense 1996), 236.

[20] Griffin.

[21] Kenneth A. Minihan, "Intelligence and Information Systems Security: Partners in Defensive Information Warfare", *Defense Intelligence Journal*, 5-1 (1996), 14.

[22] The Washington Post, "Listening To The World"; available from http://www.washingtonpost.com/wp-srv/WPlate/1997-01/31/0131-013197-idx.html; Internet accessed 10 February 1997. See also Stephen Barr, "Monitoring Service Spared in Latest Cuts"; available from http://www.washingtonpost.com/wp-srv/WPlate/1997-02/06/105L-020697-idx.html; Internet accessed 9 February 1997.

[23] Roger Hilsman, *The Cuban Missile Crisis: The Struggle Over Policy.* (Westport: Praeger, 1996), 123, 126.

[24] *The Sentinel* (Carlisle), 9 February 1997, pg A3.

[25] The White House, *A National Security Strategy.*

[26] Office of the Secretary of Defense, DSB Report, 3-1.

[27] Griffith, 84.

[28] Office of the Secretary of Defense, DSB Report, 2-13 & 14.

[29] Joint doctrine is extensive on the various components of IO/W. *Joint Publication (JP) 3-13.1 Command and Control Warfare, JP 3-51 Electronic Warfare, JP 3-53 Psychological Operations, JP 3-54 Operational Security, JP 3-55 Reconnaissance, Surveillance, Targeting, and Acquisition, JP 3-57 Civil Affairs*, and *JP 3-58 Deception Operations* all play a role in IO/W. Unfortunately, the capstone document *JP 3-13 Information Operations* , which was under development last fall, was put in a hold status pending resolution of issues which were unspecified, but probably related to a desire to expand the scope of the military definition beyond the confines of a geographic-focused concept to one grounded in cyberspace. For illustrative purposes, I have provided several service definitions.

The Army defines Information Dominance as:

> "The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary." *FM 100-6 Information Operations*, 1-9.

It further defines Information Operations as:

> "Continuous military operations within the Military Information Environment (MIE) that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; Information Operations include interacting with the Global Information Environment and exploiting or denying an adversary's information and decision capabilities." *FM 100-6 Information Operations*, 2-3.

Finally, the Army uses the joint definition of Information Warfare (see CJCSI 3210.01):

> "...Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks." *FM 100-6 Information Operations*, 2-2.

The common denominator for each of the doctrinal publications so far published is that they are rooted in what are essentially combat operations; there is little discussion of potential for compression effects from or into the other elements of power, especially in peacetime.

[30] Clarence A. Robinson Jr., "Information Warfare Demands Battlespace Visualization Grasp", *Signal* (February 1997), 19.

[31] Headquarters, Department of the Army, *Field Manual 34-130 Intelligence Preparation of the Battlefield* (Washington: July 1994).

[32] Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-0 Joint Operations*, (Washington: February 1995), p. III-1, "... Missions are assigned to subordinate commanders, not staff officers or coordination authorities."

[33] Ibid., p. III-2, "...Often, combatant commanders may be required to support the other instruments of national power as directed by national leadership."

[34] John McCain, "READY TOMORROW: DEFENDING AMERICAN INTERESTS IN THE 21ST CENTURY", (Washington: March 1996), 17.

Selected Bibliography

Arquilla, John and David Ronfeldt. "Cyberwar Is Coming !" *Comparative Strategy* 12, no 2 (1993): 141-165. Available from http://www.stl.nps.navy.mil/c4i/cyberwar.html; Internet accessed 08 October 1996.

Black, Steven K.. *A Sobering Look at the Contours of Cyberspace*. Pittsburgh: Ridgway Center for International Security Studies, 1996. Ridgway Viewpoints No. 96-3.

_____. *Information Warfare in the Post-Cold War World.* Pittsburgh: Ridgway Center for International Security Studies, 1996. Ridgway Viewpoints No. 96-1.

Larry Bond, *The Enemy Within.* New York: Warner Books, 1996.

Brock, Jack L.. *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Statement before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, US Senate, Washington, DC, 22 May 1996. GAO/T-AIMD-96-92.

_____. *Computer Security: Hackers Penetrate DOD Computer Systems*. Statement before the Subcommittee on Government Information and Regulation, Committee on Governmental Affairs, US Senate, Washington, DC, 20 May 1991. GAO/T-IMTEC-92-5.

CERT Coordination Center. "1995 Annual Report (Summary)." Carnegie Mellon University. Available from http://www.cert.org/cert.report.95.html; Internet accessed 01 October 1996.

_____. "Frequently Asked Questions." Carnegie Mellon University. Available from http://www.cert.org/cert.faqintro.html; Internet accessed 01 October 1996.

Cooper, David E., "Statement Before the Senate Select Committee on Intelligence on Economic Espionage: Information on Threat from US Allies" on 28 February 1996; available from http://nsi.org/Library/Espionage/allies.txt; Internet accessed 23 January 1997.

Drake, William J.. *The New Information Infrastructure: Strategies for US Policy*. New York: Twentieth Century Fund Press, 1995.

Fast, William R.. *Knowledge Strategies: Balancing Ends, Ways, And Means in the Information Age*. Research Project. Carlisle Barracks: US Army War College, April 1996.

Golden, James R.. *Economics and National Strategy in the Information Age: Global Networks, Technology Policy, and Cooperative Competition.* Westport: Praeger, 1994.

Griffin, Samuel B., ed,. *Sun Tzu: The Art of War* . London: Oxford University Press, 1971.

Hancock, Garth, "US Economic Intelligence Policy and Global Competition." Spring 1996; available from http://www.miis.edu/mreview/spring96/hancockart.html; Internet accessed 23 January 1997.

Roger Hilsman, *The Cuban Missile Crisis: The Struggle Over Policy.* Westport: Praeger, 1996.

Libicki, Martin C.. *What Is Information Warfare?*, Washington: National Defense University, 1995.

Libicki, Martin C., "Defending the National Information Infrastructure". Available from http://www.ndu.edu/ndu/inss/actpubs/niitemp.html; Internet accessed 21 March 1997.

Lykke, Arthur F., Jr. *Military Strategy: Theory and Application.* Carlisle Barracks, PA: U.S. Army War College, 1993.

MacGregor, Douglas A., "Future Battle: The Merging Levels of War," *Parameters* 22 Winter 1992-93.

McCain, John, "READY TOMORROW: DEFENDING AMERICAN INTERESTS IN THE 21ST CENTURY." Washington: March 1996.

Minihan, Kenneth A.. "Intelligence and Information Systems Security: Partners in Defensive Information Warfare." *Defense Intelligence Journal* 5, no. 1 (1996): 13-23.

Molander, Roger C., Andrew S. Riddle, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." *Parameters* 26, no. 3 (1996): 81-92.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson. *Strategic Information Warfare: A New Face of War.* Santa Monica: RAND, 1996.

Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy of the United States of America 1995*. Washington: U.S. Department of Defense, 1995.

Office of the Chairman of the Joint Chiefs of Staff. *Joint Vision 2010*. Washington: 1996.

Office of the Chairman of the Joint Chiefs of Staff. *Information Warfare: A Strategy for Peace...The Decisive Edge In War*. Washington: 1997.

Office of the Chairman of the Joint Chiefs of Staff. *Joint Publication 3-0 Joint Operations*. Washington: February 1995.

Office of the Chief of Staff of the Army, *Army Vision 2010*. Washington: 1996.

Office of the President of the United States. *A National Security Strategy of Engagement and Enlargement*. Washington: The White House, February 1996.

Office of the President of the United States, *Executive Order #12864: United States Advisory Council on the National Information Infrastructure*, Washington: September 1993. Available from http://library.whitehouse.gov; Internet accessed 07 October 1996.

Office of the Secretary of Defense, *Report of the Secretary of Defense to the President and the Congress*, Washington: U.S. Department of Defense, 1996.

Office of the Secretary of Defense, *Defense Science Board Task Force On Information Warfare - Defense (IW-D)*, (DSB Report), Washington: November 1996.

Robinson Jr., Clarence A., "Information Warfare Demands Battlespace Visualization Grasp." *Signal* February 1997.

Stein, George J., "Information Warfare;" Available from http://www.cdsar.af.mil/apj/stein.html; Internet accessed 02 September 1996.

Szafranski, Richard. "A Theory of Information Warfare." *Air Power Journal*. Available from http://www.cdsar.af.mil/apj/szfran.html; internet; accessed 02 September 1996.

Toffler, Alvin and Heide, *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown, 1993.

U.S. Department of the Army, *Information Operations*, FM 100-6. Washington: U.S. Department of the Army, 1996.

U.S. Department of Defense. *Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance*. Washington: U.S. Department of Defense, 1996.

U.S. National Defense University. *Strategic Assessment 1996: Instruments of U.S. Power*. Washington: Institute for National Strategic Studies, National Defense University, 1996.